2023 Session B

B1. Consider an m-by-n grid of unit squares, indexed by (i, j) with $1 \le i \le m$ and $1 \le j \le n$. There are $(m-1)(n-1)$ coins, which are initially placed in the squares (i, j) with $1 \le i \le m-1$ and $1 \le j \le n-1$. If a coin occupies the square (i, j) with $i \le m-1$ and $j \le n-1$ and the squares $(i+1, j)$, $(i, j+1)$, and $(i+1, j+1)$ are unoccupied, then a legal move is to slide the coin from (i, j) to $(i+1, j+1)$. How many distinct configurations of coins can be reached starting from the initial configuration by a (possibly empty) sequence of legal moves?

Answer: $\displaystyle\binom{m+n-2}{m-1}$

Solution 1: Think of $(1, n)$ as the northwest corner of the grid and $(m, 1)$ as the southeast corner. Consider the unoccupied squares. Initially, they consist of all the squares in the north row ($j = n$) and/or the east column ($i = m$). We think of these squares as forming a lattice path from $(1, n)$ to $(m, 1)$, and we denote this path by $\underbrace{E \dots E}_{m-1}\underbrace{S \dots S}_{n-1}$, representing the sequence of eastward and southward steps that traverse the path from northwest corner to southeast corner.

Claim. *The unoccupied squares always form a lattice path from* $(1, n)$ *to* $(m, 1)$, *with a total of* $m-1$ *eastward steps and* $n-1$ *southward steps, and all such lattice paths can be achieved by a sequence of legal moves.*

Proof. The squares $(1, n)$ and $(m, 1)$ always remain unoccupied, because no legal move can slide a coin to either square. A legal move changes an ES portion (consisting of three unoccupied squares that make the move legal) of an unoccupied lattice path to SE, so by induction, after every move the unoccupied squares continue to form a lattice path consisting of the same number of E and S steps.

On the other hand, given a lattice path of E and S steps from $(1, n)$ to $(m, 1)$, which must consist of $m+n-1$ squares, consider the configuration with coins on every square not on the path. If the sequence of steps does not contain an SE portion, then we are in the initial configuration. Otherwise, choose any SE portion; the three squares connected by the SE steps must have coordinates $(i, j+1)$, (i, j), and $(i+1, j)$, and there must be a coin in square $(i+1, j+1)$. Sliding that coin to square (i, j) is the reverse of a legal move, and changes SE to ES in the path. Continue to change instances of SE to ES in this way until the initial configuration is reached. Reversing the sequence of coin slides made yields a sequence of legal moves from the initial configuration to the given configuration. $\square$

Thus, the total number of configurations is the number of possible lattice paths, which is the number of different sequences of $m-1$ E's and $n-1$ S's; this number is $\binom{m+n-2}{m-1}$.

B2. For each positive integer n, let $k(n)$ be the number of ones in the binary representation of $2023 \cdot n$. What is the minimum value of $k(n)$?

Answer: 3

Solution 1: Clearly $k(n)$ must be more than one, since no power of 2 is a multiple of $2023 = 7 \cdot 17^2$. Furthermore, powers of 2 are all congruent to $1, 2,$ or $4 \pmod 7$, and no sum of two of these residues can be zero. So $k(n)$ must be at least three. We now show that this can be achieved.

Note that the binary representations of both prime power divisors of 2023 have exactly three ones, as $7 = 2^2+2^1+2^0$ and $17^2 = 289 = 2^8+2^5+2^0$. It is now possible to piece together three powers of 2 whose sum is simultaneously a multiple of 7 and 289 using the Chinese Remainder Theorem, since the multiplicative order of 2 modulo 7 is 3, which is coprime to $16 \cdot 17 = 272$, the order of the group of multiplication modulo 289 (from which it follows that $2^{272} \equiv 1 \pmod{289}$, by Euler/Lagrange's Theorem).

In particular, the triple $(0, 277, 8)$ is congruent to $(0, 1, 2) \pmod 3$ and $(0, 5, 8) \pmod{272}$, so $2^{277} + 2^8 + 2^0$ is a multiple of 2023. (Another natural solution here is $2^{280} + 2^5 + 2^0$.)

Solution 2: As in Solution 1, $k(n) \geq 3$ for all n. This solution gives an alternative simple approach for constructing n that achieve $k(n) = 3$.

Since $2^4 = 17 - 1$, raising both sides to the 17th power and using the binomial theorem yields $2^{68} \equiv -1 \pmod{17^2}$. Also, squaring both sides yields $2^{136} \equiv 1 \pmod{17^2}$. Since $2^{68} = 2^{67}+2^{67}$, we therefore have $2^{67}+2^{67}+2^0 \equiv 0 \pmod{17^2}$. As in Solution 1, $2^i+2^j+2^k \equiv 0 \pmod 7$ if and only if $\{i, j, k\} \equiv \{0, 1, 2\} \pmod 3$. Since $136 \equiv 1 \pmod 3$, this can be achieved by $2^{203} + 2^{67} + 2^0$, which is a multiple of 2023.

As a minor variant, we similarly have $2^{69} + 2^0 + 2^0 \equiv -2 + 1 + 1 \equiv 0 \pmod{17^2}$, which naturally leads to the following solutions: $2^{69}+2^{136}+2^{272}$, $2^{205}+2^{272}+2^0$, and $2^{341}+2^{136}+2^0$.

Solution 3: This solution provides an exhaustive description of all possible triples of non-negative integers (i, j, k) such that $2^i + 2^j + 2^k \equiv 0 \pmod{2023}$. All solutions can be reduced to a canonical form by factoring out (and removing) common powers of 2, and without loss of generality the terms may be ordered as $2^i+2^j+2^0$, where $i \geq j$. The Chinese Remainder Theorem implies that the exponents i and j may be taken as residues modulo $\text{lcm}[3, 136] = 408$ (note that the calculations in Solution 2 imply that the multiplicative order of 2 modulo 17^2 is 136; this is not necessary for the construction of single examples as in that solution, but it is needed here in order to define the shape of canonical solutions). With these restrictions, we will show that there are exactly 51 unique solutions, which are listed at the end.

In fact, all solutions lie in two simple families. Indeed, any (i, j) such that $2^i + 2^j \equiv -1 \pmod{2023}$ also projects to a solution modulo 17. The order of 2 modulo 17 is 8, and there are two solutions: $(3, 3)$ and $(5, 0)$. We now must check whether these lift to solutions modulo 17^2.

In the first case, such a lift has the form

$$2^{8\alpha+3} + 2^{8\beta+3} \equiv -1 \pmod{17^2}$$

for some integers $0 \leq \alpha, \beta \leq 16$. The Binomial Theorem implies that

$$2^{8\alpha} \equiv (15 \cdot 17 + 1)^\alpha \equiv 1 + \alpha \cdot 15 \cdot 17 \pmod{17^2}.$$

Plugging this in, the above equation reduces to

$$(8(\alpha+\beta)\cdot 15+1)\cdot 17 \equiv 0 \pmod{17^2} \iff 8(\alpha+\beta)\cdot 15+1 \equiv 0 \pmod{17},$$

which reduces to $\alpha+\beta+1 \equiv 0 \pmod{17}$. Since α, β play a symmetric role, the possible sets of solutions modulo 17^2 are spanned by choosing $0 \le \alpha \le 8$ and $\beta = 16-\alpha$. To recover solutions modulo 2023, multiples of 136 must be added to $(8\alpha+3, 8\beta+3)$ until the values are congruent to $\{1,2\} \pmod 3$. For $\alpha < 8$ there are two distinct ways of doing this, but for $\alpha = 8$ there is only one, making for 17 total solutions. (In fact, when $\alpha = 8$ we recover the congruence from Solution 2, namely $2^{67}+2^{67}+2^0 \equiv 0 \pmod{17^2}$, which lifts uniquely to $(203, 67)$).

For the case $(5,0)$, the calculations are similar. We find that $2^{8\alpha+5}+2^{8\beta} \equiv -1 \pmod{17^2}$ has solutions parameterized by $\beta = 1+2\alpha \mod 17$. Now each such pair lifts to two solutions modulo 2023, since α and β are no longer symmetric, so this gives a total of 34 solutions. For example, $\alpha = 0, \beta = 1$ corresponds to $2^5+2^8+2^0 \equiv 1 \pmod{17^2}$ from Solution 1, and $\alpha = 8, \beta = 0$ corresponds to $2^{69}+2^0+2^0$ from Solution 2.

The set of all reduced (i,j) is as follows:

$$(77,16),(85,32),(101,64),(109,80),(125,112),(133,128),(139,131),(155,115),$$
$$(160,149),(163,107),(176,157),(179,91),(187,83),(203,67),(208,173),(211,59),$$
$$(224,181),(227,43),(235,35),(251,19),(256,197),(259,11),(272,205),(277,8),$$
$$(280,5),(293,40),(296,13),(301,56),(304,221),(317,88),(320,229),(325,104),$$
$$(328,29),(341,136),(344,37),(347,331),(349,152),(352,245),(355,323),(365,184),$$
$$(368,253),(371,307),(373,200),(376,53),(379,299),(389,232),(392,61),(395,283),$$
$$(397,248),(400,269),(403,275).$$

B3. A sequence $y_1, y_2, \dots, y_k$ of real numbers is called *zigzag* if $k = 1$, or if $y_2 - y_1, y_3 - y_2, \dots, y_k - y_{k-1}$ are nonzero and alternate in sign. Let $X_1, X_2, \dots, X_n$ be chosen independently from the uniform distribution on $[0,1]$. Let $a(X_1, X_2, \dots, X_n)$ be the largest value of k for which there exists an increasing sequence of integers $i_1, i_2, \dots, i_k$ such that $X_{i_1}, X_{i_2}, \dots X_{i_k}$ is zigzag. Find the expected value of $a(X_1, X_2, \dots, X_n)$ for $n \geq 2$.

Answer: $(2n+2)/3$ for $n \geq 2$.

Solution 1: We begin by noting that with probability one, the X_i are all distinct. Indeed, the event in which there are at least two identical values defines a finite collection of hyperplanes in $[0,1]^n$, which has measure zero. Furthermore, since we consider only relative order , we can translate the problem to computing $a(w)$, where $w = w_1 \dots w_n$ is a permutation of $[1, \dots, n]$ chosen uniformly at random.

Let $u(w)$ be the length of maximal zigzag sequence starting with a descent, and let $d(w)$ be the maximal zigzag sequence starting with an ascent. Then $a(w) = \max\{u(w), d(w)\}$ and moreover, for $n \geq 2$ we see that $u(w) = d(w) \pm 1$, as we can obtain one from the other by adding/removing an initial element. By symmetry we see that $u(w)$ and $d(w)$ are identically distributed and exactly half of the time $u(w)$ will be the larger. Thus, by linearity of expectation, we have

$$\mathbf{E}[a(w)] = \mathbf{E}[u(w)] + \frac{1}{2}\mathbf{E}[1] = \mathbf{E}[u(w)] + \frac{1}{2} = \mathbf{E}[d(w)] + \frac{1}{2}.$$

We claim that a maximal zigzag subsequence can always be chosen containing the value n. If a zigzag subsequence has $w_r = n$ where $i_j < r < i_{j+1}$, then we can reassign $i_j = r$ if $w_{i_j} > w_{i_{j+1}}$ or $i_{j+1} = r$ if $w_{i_j} < w_{i_{j+1}}$, resulting either way in a zigzag subsequence of the same length containing n. If $r < i_1$, we can reassign $i_1 = r$ if $w_{i_1} > w_{i_2}$ or prepend w_r to w_{i_1} if $w_{i_1} < w_{i_2}$, resulting an a zigzag subsequence of the same length or longer. The case $r > i_k$, where k is the length of the subsequence, is similar.

Let S_n denote the permutations of $[1, \dots, n]$, and define

$$f_n := \mathbf{E}[d(w) | w \in S_n], \qquad g_n := \mathbf{E}[a(w) | w \in S_n].$$

By the above reasoning we have $g_n = f_n + \frac{1}{2}$.

Let $w \in S_{n+1}$. By the above reasoning, we can assume that the element $n+1$ is part of a maximal zigzag sequence $w_{i_1} \cdots w_{i_k}$. Suppose that $w_{j+1} = n+1$ and $i_r = j+1$. Then $w_{i_{r-1}} < w_{i_{r-2}} > \cdots$ is a maximal UD alternating subsequence (i.e. starting with an ascent) in the reverse permutation $w_j \dots w_1$, and $w_{i_{r+1}} < w_{i_{r+2}} > \cdots$ is a maximal UD alternating subsequence in $w_{j+2} \dots w_{n+1}$. Thus we see that, choosing j with probability $\frac{1}{n+1}$, we have

$$g_{n+1} = \frac{1}{n+1} \sum_{j=0}^{n} (f_j + f_{n-j} + 1).$$

We have the following boundary values, which are verified directly: $f_0 = 0$, $f_1 = 1$, $f_2 = \frac{3}{2}$ ($d(12) = 2$ and $d(21) = 1$).

Then

$$g_{n+1} = f_{n+1} + \frac{1}{2} = \frac{1}{n+1} \left(2f_0 + 2f_1 + 2\sum_{j=2}^{n} f_j \right) + 1$$

Rewriting this recursion for f we get

$$f_{n+1} = \frac{2}{n+1}\left(1 + \sum_{j=2}^{n} f_j\right) + \frac{1}{2}.$$

Note that this implies a relation of $f_2 + \cdots + f_n$ via f_{n+1}, which can be then reiterated for $n-1$ and substituted

$$\frac{n+1}{2}\left(f_{n+1} - \frac{1}{2}\right) = 1 + f_2 + \cdots + f_{n-1} + f_n \Longrightarrow \frac{n+1}{2}\left(f_{n+1} - \frac{1}{2}\right) = \frac{n}{2}\left(f_n - \frac{1}{2}\right) + f_n$$

Then

$$(n+1)f_{n+1} = (n+2)f_n + \frac{1}{2} \Longrightarrow (n+1)\left(g_{n+1} - \frac{1}{2}\right) = (n+2)\left(g_n - \frac{1}{2}\right) + \frac{1}{2},$$

so

$$(n+1)g_{n+1} = (n+2)g_n \Longrightarrow \frac{g_{n+1}}{n+2} = \frac{g_n}{n+1} = \cdots = \frac{g_2}{3} = \frac{2}{3},$$

which completes the proof.

Solution 2: The event that two of the X_j's are equal has probability zero, so in the argument below we assume that no two are equal. For $1 < j < n$, call j a "turning point" if $X_j - X_{j-1}$ and $X_{j+1} - X_j$ have opposite signs, and let T be the total number of turning points.

We claim that $a(X_1, \ldots, X_n) = T + 2$. For $1 \le j < n$, let $D_j = X_{j+1} - X_j$. Suppose that $X_{i_1}, \ldots, X_{i_k}$ is zigzag. For each $1 \le m < k$, we have $X_{i_{m+1}} - X_{i_m} = D_{i_m} + D_{i_m+1} + \cdots + D_{i_{m+1}-1}$. Choose ℓ_m with $i_m \le \ell_m < i_{m+1}$ so that D_{ℓ_m} has the same sign as $X_{i_{m+1}} - X_{i_m}$. Then the sequence $D_{\ell_1}, D_{\ell_2}, \ldots, D_{\ell_{k-1}}$ alternates sign. Thus, there are at least $k-2$ changes of sign in the sequence $D_1, D_2, \ldots, D_{n-1}$. Each such change of sign is a turning point, so $k - 2 \le T$, and $k \le T + 2$. To see that $k = T + 2$ is possible, let $j_1, j_2, \ldots, j_T$ be the turning points. Then $D_1, D_2, \ldots, D_{n-1}$ changes sign only between D_{j_m} and $D_{j_m - 1}$ for $m = 1, 2, \ldots, T$. It follows that the sequence

$$\begin{aligned} &X_{j_1} - X_1, X_{j_2} - X_{j_1}, \ldots, X_{j_T} - X_{j_{T-1}}, X_n - X_{j_T} \\ &\quad = D_1 + \cdots + D_{j_1 - 1}, Dj_1 + \cdots + D_{j_2 - 1}, \ldots, D_{j_{T-1}} + \cdots + D_{j_T - 1}, D_{j_T} + \cdots + D_{n-1} \end{aligned}$$

alternates sign, so $X_1, X_{j_1}, \ldots, X_{j_T}, X_n$ is a zigzag subsequence with length $T + 2$. This verifies our claim.

For $1 < j < n$, the probability that j is a turning point is $2/3$, since 4 of the 6 equally likely orderings of X_{j-1}, X_j, X_{j+1} yield a turning point. Therefore, $\mathbf{E}[a(X)] = (n-2)2/3 + 2 = (2n+2)/3$.

Solution 3: Let $Z_j = a(X_1, \ldots, X_j) - a(X_1, \ldots, X_{j-1})$ for $j \ge 3$. Then for $n \ge 2$, we can write $a(X_1, \ldots, X_n) = a(X_1, X_2) + Z_3 + \cdots + Z_n$, so it suffices to determine

$$\mathbf{E}[a(X_1, X_2) + Z_3 + \cdots + Z_n] = \mathbf{E}[a(X_1, X_2)] + \mathbf{E}[Z_3] + \cdots \mathbf{E}[Z_n].$$

Notice that $\mathbf{E}[a(X_1, X_2)] = 2$ since with probability one either $X_1 > X_2$ or $X_1 < X_2$, and in either case X_1, X_2 is zigzag. We claim that $\mathbf{E}[Z_j] = 2/3$ for $j \ge 3$, from which the answer $2 + 2(n-2)/3 = (2n+2)/3$ follows immediately.

To verify the claim, we first excluded the possibility that two of the X_i's are equal, which has probability zero. Next, notice that if $X_{i_1}, \dots, X_{i_k}$ is zigzag and $i > i_k$, then either $X_{i_1}, \dots, X_{i_{k-1}}, X_i$ or $X_{i_1}, \dots, X_{i_k}, X_i$ is zigzag, according (if $k \geq 2$) to whether or not X_{i_k} is between $X_{i_{k-1}}$ and X_i. Then if $k = a(X_1, \dots, X_{j-1})$ and $X_{i_1}, \dots, X_{i_k}$ is zigzag, $X_{i_1}, \dots, X_{i_{k-1}}, X_{j-1}$ must also be zigzag (since otherwise there would be a longer zigzag subsequence). Further, $X_{j-1} - X_{j-2}$ must have the same sign as $X_{j-1} - X_{i_{k-1}}$; otherwise, $X_{j-2} - X_{i_{k-1}} = (X_{j-2} - X_{j-1}) + (X_{j-1} - X_{i_{k-1}})$ would have the same sign as $X_{j-2} - X_{j-1}$ and $X_{j-1} - X_{i_{k-1}}$, hence the opposite sign as $X_{j-1} - X_{j-2}$, making a longer zigzag subsequence $X_{i_1}, \dots, X_{i_{k-1}}, X_{j-2}, X_{j-1}$. Thus, $Z_j = 0$ if $X_j - X_{j-1}$ has the same sign as $X_{j-1} - X_{j-2}$, and $Z_j = 1$ if they have opposite signs. In other words, $Z_j = 0$ if X_{j-1} is between X_{j-2} and X_j, and $Z_j = 1$ otherwise. Since X_{j-1} is between X_{j-2} and X_j for 2 of the 6 equally likely orderings of X_{j-2}, X_{j-1}, X_j, the probability that $Z_j = 1$ is $4/6 = 2/3$, and $\mathbf{E}[Z_j] = 2/3$ as claimed.

B4. For a nonnegative integer n and a strictly increasing sequence of real numbers $t_0, t_1, \ldots, t_n$, let $f(t)$ be the corresponding real-valued function defined for $t \geq t_0$ by the following properties:

(a) $f(t)$ is continuous for $t \geq t_0$, and is twice differentiable for all $t > t_0$ other than $t_1, \ldots, t_n$;

(b) $f(t_0) = 1/2$;

(c) $\lim_{t \to t_k^+} f'(t) = 0$ for $0 \leq k \leq n$;

(d) For $0 \leq k \leq n-1$, we have $f''(t) = k+1$ when $t_k < t < t_{k+1}$, and $f''(t) = n+1$ when $t > t_n$.

Considering all choices of n and $t_0, t_1, \ldots, t_n$ such that $t_k \geq t_{k-1} + 1$ for $1 \leq k \leq n$, what is the least possible value of T for which $f(t_0 + T) = 2023$?

Answer: 29

Solution 1: Let T be the value for which $f(t_0 + T) = 2023$, and assume without loss of generality that $t_n < t_0 + T$, since greater values do not affect $f(t_0 + T)$. Let $t_{n+1} = t_0 + T$. Notice that for each $1 \leq k \leq n+1$ we have $f(t) = f(t_{k-1}) + k(t - t_{k-1})^2/2$ when $t_{k-1} \leq t \leq t_k$. Let $\tau_k = t_k - t_{k-1}$; then $\tau_k \geq 1$ for $1 \leq k \leq n$ and $\tau_{n+1} \geq 0$. Let $m = n+1$. The goal is to minimize $T = \tau_1 + \tau_2 + \cdots + \tau_m$ subject to the constraint

$$C(\tau) := \sum_{k=1}^{m} k\tau_k^2 = 2(f(t_0 + T) - f(t_0)) = 4045.$$

The space to be minimized over consists of all $m \geq 1$ and all real m-tuples $(\tau_1, \ldots, \tau_m)$ with $\tau_k \geq 1 - \delta_{mk}$, where δ_{mk} is the Kronecker delta. This space can be made topologically connected with the identification $(\tau_1, \ldots, \tau_{m-1}, 0) = (\tau_1, \ldots, \tau_{m-1})$ for $m \geq 2$. The subset of this space that satisfies the constraint is bounded and hence compact, because the constraint excludes values of m for which $m(m-1)/2 > 4045$ and values of τ_k greater than $\sqrt{4045}$.

Let $(\tau_1, \tau_2, \cdots, \tau_m)$ lie in the constrained space, so that $C(\tau) = 4045$ and $\tau_k \geq 1 - \delta_{mk}$. If there is more than one value of k for which $\tau_k > 1 - \delta_{mk}$, let two of these values be k_1 and k_2, and assume without loss of generality that $k_1\tau_{k_1} \geq k_2\tau_{k_2}$. Choose $\varepsilon > 0$ sufficiently small that $\tau_{k_2} - \varepsilon \geq 1 - \delta_{mk_2}$, and consider the m-tuple for which (τ_{k_1}, τ_{k_2}) is replaced by $(\tau_{k_1} + \varepsilon, \tau_{k_2} - \varepsilon)$, and the other τ_k are unchanged. Then T is unchanged, while the sum $\sum_{k=1}^{m} k\tau_k^2$ in the constraint changes by

$$2(k_1\tau_{k_1} - k_2\tau_{k_2})\varepsilon + (k_1 + k_2)\varepsilon^2,$$

which is (strictly) positive by our earlier assumption. Thus, the sum is now greater than 4045. Next, reduce $\tau_{k_1} + \varepsilon$ until the constraint is satisfied again, and notice that the value that meets this condition is strictly between τ_{k_1} and $\tau_{k_1} + \varepsilon$ (since $C(\tau)$ is increasing in each τ_k), so it satisfies the same lower bound as τ_{k_1}. The resulting m-tuple has a strictly lower value of T, so the original m-tuple could not have minimized T. Thus, the (constrained) minimum of T cannot be achieved with more than one value of k for which $\tau_k > 1 - \delta_{mk}$.

Next, suppose that T is minimized with $\tau_k > 1$ for some $k < m$; then by the argument above, $\tau_m = 0$. In that case, reduce m by 1, and since $\tau_{m-1} > 0$, the above argument implies

that T is not at a minimum for the new value of m, and hence not a global minimum. By the compactness described above, there must be a global minimum value for T, and by what we have argued so far, this minimum must satisfy $\tau_1 = \tau_2 = \cdots = \tau_{m-1} = 1$. Thus, the problem is reduced to minimizing

$$T(m) = m - 1 + \sqrt{\left(4045 - \sum_{k=1}^{m-1} k\right) / m} = m - 1 + \sqrt{4045/m - (m-1)/2}$$

over all $1 \le m \le M$, where M is the greatest integer for which the square root is well-defined. The fact that $M \ge 20$ suffices for the arguments below.

If $m < M$, then $T(m+1) > T(m)$ is equivalent to

$$1 + \sqrt{4045/(m+1) - m/2} > \sqrt{4045/m - (m-1)/2}.$$

Squaring both sides (which we observe are nonnegative) and simplifying, this is equivalent to

$$2\sqrt{4045/(m+1) - m/2} > 4045/[m(m+1)] - 1/2.$$

Notice that the right side is nonnegative when the left side is well-defined (when $m < M$). We square and simplify again to conclude that $T(m+1) > T(m)$ is equivalent to

$$4m > 4045/[m(m+1)] - 1/2 \iff m(m+1)(m+1/8) > 1011.25.$$

Thus, $T(m+1) > T(m)$ for $10 \le m < M$.

Similarly, $T(m+1) < T(m)$ is equivalent to $m(m+1)(m+1/8) < 1011.25$, which is true for $1 \le m \le 9$. We conclude that $T(10) = 9 + \sqrt{404.5 - 4.5} = 29$ is the minimum possible value of T.

Solution 2: Following the same notation and initial steps as the previous solution, the goal is to minimize $T = \tau_1 + \tau_2 + \cdots + \tau_{n+1}$ subject to the constraint

$$C(\tau) := \sum_{k=1}^{n+1} k\tau_k^2 = 4045,$$

where $n \ge 0$ and $\tau_k \ge 1$ for $k = 1, \dots, n$ and $\tau_{n+1} \ge 0$.

We now make the following substitution: Let $x_k = k\tau_k^2 - k \ge 0$ for $k = 1, \dots, n$ and $x_{n+1} = (n+1)\tau_{n+1}^2$. We have $x_i \ge 0$ and

$$x_{n+1} = 4045 - \binom{n+1}{2} - x_1 - \cdots - x_n \ge 0.$$

Then the goal is to minimize

$$F_n(x_1, \dots, x_n) := \sum_{k=1}^{n} \sqrt{\frac{x_k + k}{k}} + \sqrt{\frac{4045 - \binom{n+1}{2} - x_1 - \cdots - x_n}{n+1}}$$

over the simplex $x_i \ge 0$ and $x_1 + \cdots + x_n \le 4045 - \binom{n+1}{2}$, and over $n \ge 0$ for which this simplex is non-empty. (We include $n = 0$, for which the simplex is undefined but the original constraint requires $\tau_1 = 4045$; in this case, $T = \sqrt{4045}$, so we let $F_0 = \sqrt{4045}$.)

We now analyze the function $g_k(x_k) = F_n(x_1, \ldots, x_n)$ for fixed values of x_j, $j \neq k$. We have

$$g_k'(x_k) = \frac{1}{2\sqrt{k(x_k+k)}} - \frac{1}{2\sqrt{(n+1)\left(4045 - \binom{n+1}{2} - x_1 - \cdots - x_n\right)}}$$

$$g_k''(x_k) = -\frac{1}{4\sqrt{k}(x+k)^{3/2}} - \frac{1}{4\sqrt{n+1}\left(4045 - \binom{n+1}{2} - x_1 - \cdots - x_n\right)^{3/2}} < 0,$$

so g_k is a concave function and the minimum is achieved at the boundary. Thus we either have $x_k = 0$ or $x_1 + \cdots + x_n = 4045 - \binom{n+1}{2}$ for every k. So the minimum is achieved for some $(x_1, \ldots, x_n)$ either on the hyperplane $H_n := \{x_1 + \cdots + x_n = 4045 - \binom{n+1}{2}\}$ or else we must have $x_k = 0$ for all k so $(x_1, \ldots, x_n) = (0, \ldots, 0)$.

In the first case we have $x_n = 4045 - \binom{n+1}{2} - x_1 - \cdots - x_{n-1}$, so

$$F_n(x_1, \ldots, x_n) = \sum_{k=1}^{n-1} \sqrt{\frac{x_k+k}{k}} + \sqrt{\frac{4045 - \binom{n+1}{2} - x_1 - \cdots - x_{n-1} + n}{n}} = F_{n-1}(x_1, \ldots, x_{n-1}).$$

If $(x_1, \ldots, x_{n-1})$ minimizes F_{n-1} and $(x_1, \ldots, x_{n-1}) \in H_{n-1}$, then we can again reduce to the case of one fewer variable. Recursively, we can eventually reach a minimum in the second case where $(x_1, \ldots, x_N) = (0, \ldots, 0)$, which is vacuously true for $N = 0$ in case we get that far.

Having reduced to the second case, we now need only minimize the function

$$t(N) := f_N(0, \ldots, 0) = N + \sqrt{\frac{4045 - \binom{N+1}{2}}{N+1}} = N + \sqrt{\frac{4045}{N+1} - \frac{N}{2}}$$

over the integers $0 \leq N \leq 89$ (since the square root is undefined for $N \geq 90$). To motivate the next steps, crude estimates show that $t(1) > 40$, $t(3) < 40$, $t(10) < 40$, and $t(30) > 40$. This suggests that the minimum occurs when $\frac{4045}{N+1}$ is considerably larger than $\frac{N}{2}$. To get a rough idea where the minimum occurs, replace N for the moment with a real variable y, and consider the approximation $t(y) \approx y + \sqrt{\frac{4045}{y+1}}$. From its derivative, the latter function is minimized when $y = -1 + (4045/4)^{1/3} \approx 9$.

Consider then $t(y) - t(9) = t(y) - 29$; we will find values of $y \geq 0$ for which this is nonpositive. Thus, we are solving for

$$\sqrt{\frac{4045}{y+1} - \frac{y}{2}} \leq 29 - y \iff y \leq 29 \text{ and } \frac{4045}{y+1} - \frac{y}{2} \leq (29-y)^2.$$

The last inequality is equivalent to (using the fact that we have equality for $y = 9$ to factor)

$$\begin{aligned}(y-29)^2(y+1) - 4045 + \frac{y(y+1)}{2} &= 1/2(y-9)(2y^2 - 95y + 712) \\ &= \frac{1}{4}(y-9)\left(y - \frac{95+\sqrt{3329}}{4}\right)\left(y - \frac{95-\sqrt{3329}}{4}\right) \geq 0.\end{aligned}$$

This inequality is true only when $y \geq \frac{95+\sqrt{3329}}{4} > 29$ or when y is (not strictly) between 9 and $\frac{95-\sqrt{3329}}{4}$. The latter number is strictly between 9 and 10 because $55^2 = 3025 < 3329 < 3481 = 59^2$. Thus, $t(y) - t(9) \leq 0$ only when $9 \leq y \leq \frac{95-\sqrt{3329}}{4} < 10$. Then $t(N) \geq t(9)$ for integers N, and $t(9) = 29$ is the desired minimum.

B5. Determine which positive integers n have the following property: For all integers m that are relatively prime to n, there exists a permutation $\pi : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ such that $\pi(\pi(k)) \equiv mk \pmod{n}$ for all $k \in \{1, 2, \dots, n\}$.

Answer: Those n of the form $4j + 2$ where j is a nonnegative integer, and $n = 1$.

Solution: Suppose that $\tau \in S_n$, where S_n is the group of permutations on n elements. We say that a permutation $\pi \in S_n$ is a *square root* of τ if $\pi^2 = \tau$ (we will shortly see that in general there is not a unique square root, if one exists). If m is an integer coprime to n, let $\tau_m \in S_n$ denote the permutation defined by multiplication by m modulo n, in other words, $\tau_m(k) = m \cdot k \mod n$ for $1 \le k \le n$. The problem statement asks for a classification of the n such that *all* τ_m have a square root in S_n.

Now consider the standard decomposition of τ into disjoint cycles. For a positive integer i such that $i \le n$, let $f_i(\tau)$ denote the number of distinct cycles of length i.

Lemma. *Suppose that $\tau \in S_n$. Then τ has a square root if and only if $f_{2i}(\tau)$ is even for all $i \le \frac{n}{2}$.*

Proof. If ℓ is a positive integer, consider the permutation in S_n defined by a cycle of length ℓ, say $\gamma = (x_1 x_2 \cdots x_\ell)$. When squared, the resulting permutation either preserves the cycle length, or splits it into two cycles of half the length, depending on the parity of ℓ:

$$\gamma^2 = \begin{cases} (x_1 x_3 \cdots x_{2k+1} x_2 x_4 \cdots x_{2\lambda}) & \text{if } \ell = 2\lambda + 1, \\ (x_1 x_3 \cdots x_{2\lambda-1})(x_2 x_4 \cdots x_{2\lambda}) & \text{if } \ell = 2\lambda. \end{cases} \tag{3}$$

Applying this fact to the cycle decomposition of a permutation $\pi \in S_n$ implies that (noting that all of the resulting cycles remain disjoint)

$$\begin{aligned} f_{2\lambda+1}(\pi^2) &= f_{2\lambda+1}(\pi) + 2 f_{4\lambda+2}(\pi), \\ f_{2\lambda}(\pi^2) &= 2 f_{4\lambda}(\pi). \end{aligned}$$

Here we set $f_i(\pi) = 0$ if $i > n$. The forward direction of the claim follows, as $f_i(\pi^2)$ is even for all even i.

For the reverse direction, suppose that τ is a permutation such that $f_{2i}(\tau)$ is even for all i. We now construct a square root π as a list of cycles, essentially using (3) in reverse. For each cycle in τ of odd length, say $\gamma = (x_1 x_2 \cdots x_{2\lambda+1})$, append the following length $2\lambda + 1$ cycle to π:

$$(x_1 x_{\lambda+2} x_2 x_{\lambda+3} x_3 \cdots x_{2\lambda+1} x_{\lambda+1}).$$

By assumption, there are an even number of cycles of even length in τ, so they may be grouped (arbitrarily) in pairs. For each pair of the form $(x_1 x_2 \cdots x_{2\lambda}), (y_1 \cdots y_{2\lambda})$, append the following cycle of length 4λ to π:

$$(x_1 y_1 x_2 y_2 \cdots x_{2\lambda} y_{2\lambda}).$$

Now it is immediate that $\pi^2 = \tau$, since by construction they share the same cycle decomposition.

□

This result also shows that even parity of τ is a necessary condition for the existence of a square root (though not sufficient, as for example, $\tau = (12)(3456)$ is an even permutation without a square root).

Corollary. *If τ is an odd permutation, then it has no square root.*

Returning to the problem at hand, note that the cycles of $\tau_m \in S_n$ are of the form

$$\langle m \rangle \cdot x := (x\ mx\ \cdots m^{\ell-1}x),$$

where x is a positive integer, and ℓ is the minimum positive exponent such that $m^\ell x \equiv x \pmod{n}$. This is equivalent to the minimal ℓ such that $m^\ell \equiv 1 \pmod{\frac{n}{\gcd(x,n)}}$.

If $n = 4k+2$, then consider an arbitrary value of m, which must be odd. In this case, we will show that $f_i(\tau_m)$ is even for all i, and therefore τ_m has a square root by the Lemma. Specifically, we claim that $f_i(\tau_m) = 2o_i(\tau_m)$, where $o_i(\tau_m)$ denotes the number of cycles of length i such that all elements are odd.

To verify this claim, suppose that x is odd. Then $\langle m \rangle \cdot x$ consists of only odd integers (and any such cycle is generated by some odd x), and maps bijectively to $\langle m \rangle \cdot 2x$ (a cycle with only even integers), since $x \mapsto 2x \pmod{n}$ bijectively maps the odd residues modulo n to the even residues (noting that n is divisible by 2 but no higher power of 2).

If $n = 1$, then the property trivially holds because all integers are congruent to each other modulo 1, and because there does exist a (trivial) permutation $\pi\colon \{1\} \to \{1\}$.

For all other n, we will provide a value $m = m_n$ such that τ_{m_n} does not have a square root in S_n. If $n = 4k$, let $m_n = -1$. Then $f_1(\tau_m) = 2$ (the fixed points being $x = 0$ and $2k$) and $f_2(\tau_m) = 2k-1$, so the conclusion follows by the Lemma. A similar argument also shows that τ_{-1} does not have a square root if $n = 4k+3$. However, this does not work for $n = 4k+1$, and the case that n is odd can be treated in a unified manner as follows.

Suppose that $n > 1$ is odd, with prime factorization $n = p_1^{e_1} \cdots p_r^{e_r}$, where the p_i are distinct odd primes, and e_i are positive integers. Let m_1 be a primitive root of the multiplicative group modulo $p_1^{e_1}$ (cf. Euler, Lagrange, Legendre, Gauss for the existence of such a root). Then m_1 is also a primitive root modulo p_1^e for $1 \le e \le e_1 - 1$. Now (using the Chinese Remainder Theorem) set m to be the residue modulo n that satisfies

$$m \equiv m_1 \pmod{p_1^{e_1}}, \quad m \equiv 1 \pmod{p_j^{e_j}} \text{ for } 2 \le j \le r.$$

Then all non-fixed-point cycles of τ_m have lengths of the form $p_1^{e-1}(p_1-1)$ for some $1 \le e \le e_1$. Specifically, if x is a multiple of $p_1^{e_1}$, then $\langle a \rangle \cdot x$ has length 1, and otherwise if p_1^s is the largest power of p_1 dividing x (where $0 \le s \le e_1 - 1$), then the length is $p_1^{e_1-s-1}(p_1-1)$.

Thus by considering the cycles formed by all x's that are not multiples of p_1 (this is the case $s = 0$, but in fact any $s < e_1$ works similarly), we find that

$$f_{p_1^{e_1-1}(p-1)}(\tau_m) = \frac{n\left(1 - \frac{1}{p_1}\right)}{p_1^{e_1-1}(p_1-1)} = p_2^{e_2} \cdots p_r^{e_r}.$$

Since this is odd, the Lemma implies that τ_m is not a square.

Remark. The Corollary can also be proven directly (almost immediately using the fact that the sign map is a homomorphism). This gives an alternative criterion for showing that τ_{-1} does not have a square root when $n \equiv 0, 3 \pmod 4$.

There are many possible constructions for permutation square roots in the case $n = 4k+2$. The proof above implicitly defines a square root of τ_m by "zipping" together all cycles of the form $(x, mx, m^2x, \dots)$ and $(2x, m \cdot 2x, m^2 \cdot 2x, \dots)$. One alternative is to instead pair cycles of the form $(x, mx, m^2x, \dots)$ and $((x+n'), m(x+n'), m^2(x+n'), \dots)$, where $n' = 2k+1 = \frac{n}{2}$. To be more precise, it is straightforward to show that the following permutation is also a square root of τ_m:

$$\pi(x) := \begin{cases} x + n' \pmod n & \text{if } x \text{ is odd,} \\ mx + n' \pmod n & \text{if } x \text{ is even.} \end{cases}$$

B6. Let n be a positive integer. For i and j in $\{1,2,\ldots,n\}$, let $s(i,j)$ be the number of pairs (a,b) of nonnegative integers satisfying $ai+bj=n$. Let S be the n-by-n matrix whose (i,j)-entry is $s(i,j)$.

For example, when $n=5$, we have $S=\begin{bmatrix} 6 & 3 & 2 & 2 & 2 \\ 3 & 0 & 1 & 0 & 1 \\ 2 & 1 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 1 \\ 2 & 1 & 1 & 1 & 2 \end{bmatrix}$.

Compute the determinant of S.

Answer: $(-1)^{m+1}2m$ where m is the least integer greater than or equal to $n/2$

Solution 1: Let $d(i,j)=1$ if $i \mid j$ and 0 otherwise, and let $D=(d(i,j))_{(i,j)=(1,0)}^{(n,n)}$ be the corresponding $n\times(n+1)$ matrix whose rows are indexed by $1,\ldots,m$ and whose columns are indexed by $0,1,\ldots,n$. For example, for $n=8$, we have

$$D=\begin{pmatrix} & j=0 & j=1 & j=2 & j=3 & j=4 & j=5 & j=6 & j=7 & j=8 \\ i=1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ i=2 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ i=3 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ i=4 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ i=5 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ i=6 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ i=7 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ i=8 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

All possible solutions (a,b) to $ai+bj=n$ in nonnegative integers can be indexed by those $0\le k\le n$ such that $i\mid k$ and $j\mid n-k$, so

$$s(i,j)=\sum_{k=0}^{n} d(i,k)d(j,n-k).$$

Thus $S=D(D^r)^T$, where D^r is the matrix D with the rows reversed, i.e., $D^r_{i,j}=D_{i,n-j}$.

The Cauchy–Binet formula implies that if M is an $n\times(n+1)$-matrix and N is an $(n+1)\times n$-matrix, then

$$\det(MN)=\sum_{k=0}^{n}\det\left(M_{\widehat{k}}\right)\cdot\det\left(N^{\widehat{k}}\right),$$

where $M_{\widehat{k}}$ denotes the matrix M with the k-th column removed, and $N^{\widehat{k}}$ denotes the matrix N with the k-th row removed.

In the present case we have $M=D$ and $N=(D^r)^T$, and can further reduce

$$\det\left(\left((D^r)^T\right)^{\widehat{k}}\right)=\det\left((D^r)_{\widehat{k}}\right)=(-1)^{\lfloor n/2\rfloor}\det D_{\widehat{n-k}}.$$

The first equality is due to the fact that determinants are preserved by transposition, and the sign arises from writing the row reversals as $\lfloor n/2\rfloor$ column swaps. In all, we therefore have

$$\det S=\sum_{k=0}^{n}\det D_{\widehat{k}}(-1)^{\lfloor n/2\rfloor}\det D_{\widehat{n-k}}. \tag{4}$$

This sum can be further simplified by evaluating $\det D_{\widehat{k}}$ for large k.

Lemma. *(a) If $k > n/2$, then* $\det D_{\widehat{k}} = (-1)^{k-1}$.

(b) If n is even, then $\det D_{\widehat{n/2}} = 0$.

Proof. For $k > n/2$ we can compute $\det D_{\widehat{k}}$ by cofactor expansion along row k. For such a k we have $d(k,j) = 0$ unless $j = 0$ or k, and on removing column k, row k of $D_{\widehat{k}}$ is $[1, 0, \ldots, 0]$. Thus $\det D_{\widehat{k}} = (-1)^{k-1}$, since after removing row k and columns 0 and k of D, the remaining matrix is upper triangular with 1s on the diagonal.

If n is even, say $n = 2m$, then row m of $D_{\widehat{m}}$ is $[1, 0, \ldots, 0, 1]$ (since $d(m,j) = 1$ only when $j = 0, m, 2m$, and $j = m$ has been removed). Thus $d(m,j) = d(2m,j)$ for $j \neq m$, and since row m and row $n = 2m$ are then identical, $\det D_{\widehat{m}} = 0$. □

Plugging in to (4), we can hence in all cases set $m := \lceil n/2 \rceil$ and write

$$\det S = 2(-1)^{\lfloor n/2 \rfloor} \sum_{k=0}^{m-1} \det D_{\widehat{k}} \det D_{\widehat{n-k}} = 2(-1)^{\lfloor n/2 \rfloor} \sum_{k=0}^{m-1} (-1)^{n-k-1} \det D_{\widehat{k}}$$
$$= 2(-1)^{m-1} \sum_{k=0}^{m-1} (-1)^k \det D_{\widehat{k}},$$

where we have also used that $n - m = \lfloor n/2 \rfloor$. The proof is complete on evaluating this sum.

Claim. *We have*

$$\sum_{k=0}^{m-1} (-1)^k \det\left(D_{\widehat{k}}\right) = m.$$

Proof. Let D' be the $(n+1) \times (n+1)$-matrix obtained from D by attaching an extra row $(1, 1, \ldots, 1)$ at the top of the matrix (i.e., at row index $i = 0$). Then, the topmost two rows of the matrix D' are equal, so that $\det(D') = 0$. On the other hand, expanding the determinant of D' along the topmost row, and using part (b) of the Lemma to eliminate the middle term of the sum when n is even, we obtain

$$\det\left(D'\right) = \sum_{k=0}^{n} (-1)^k \det\left(D_{\widehat{k}}\right) = \sum_{k=0}^{m-1} (-1)^k \det\left(D_{\widehat{k}}\right) + \sum_{k=n-m+1}^{n} (-1)^k \det\left(D_{\widehat{k}}\right)$$
$$= \sum_{k=0}^{m-1} (-1)^k \det\left(D_{\widehat{k}}\right) + \sum_{k=n-m+1}^{n} (-1)^k \cdot (-1)^{k-1} = \sum_{k=0}^{m-1} (-1)^k \det\left(D_{\widehat{k}}\right) - m.$$

The second line follows by part (a) of the Lemma. Recalling that $\det(D') = 0$, the proof is complete. □

Solution 2: As in Solution 1, the $(i,j)-$th entry of S is the convolution of indicator series for multiples of i and j. In particular, this gives the factorization $S = B \cdot \mathrm{Rev}(B)^T$, where $\mathrm{Rev}(B)$ denotes the matrix formed by reversing each row of B, and B consists of the rows $R_1, \ldots, R_n$, where

$$R_i = (1\, \underbrace{0 \cdots 0}_{i-1}\, 1\, \underbrace{0 \cdots 0}_{i-1}\, 1 \cdots) = (\mathbb{1}(i \mid j))_{j=0}^{n}.$$

The key idea in this proof is to apply row operations directly on B. In particular, if M is an $n \times n$ matrix with $\det(M) = 1$, then

$$\det\left(MB \cdot \mathrm{Rev}(B)^T M^T\right) = \det(S).$$

Furthermore, $\mathrm{Rev}(B)^T M^T = \mathrm{Rev}(MB)^T$, since under left-multiplication M acts as row operations on B, which are commutative with row reversal.

The preceding claims can also be justified more explicitly by noting that $\mathrm{Rev}B = M \cdot J$, where

$$J := \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ \vdots & \iddots & & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}.$$

For example, commutativity follows since $M \cdot \mathrm{Rev}(B) = M \cdot B \cdot J = \mathrm{Rev}(MB)$.

The rows R_i form a full rank system, since B excluding the first column is upper triangular. We can therefore reduce B to the canonical form

$$MB = \begin{pmatrix} a_1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ a_2 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & & & & & & \vdots \\ a_{n-1} & 0 & 0 & 0 & \cdots & 1 & 0 \\ a_n & 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

by a sequence of row operations that acts on the rows from bottom to top, with each operation subtracting a row from below the row being acted on. It follows that a_i can be defined recursively for $i = n, n-1, \ldots, 1$ by the formula

$$a_i = 1 - a_{2i} - a_{3i} - \cdots,$$

where for convenience we set the initial conditions $a_i = 0$ for $i > n$. Equivalently, we can set additional initial conditions $a_{n-m+1}, \ldots, a_n = 1$, where $m = \lceil \frac{n}{2} \rceil$, and define a_i recursively for $i = n-m, \ldots, 1$.

Assume now that n is odd, so that $n = 2m-1$; it will turn out that $n = 2m$ reduces to

this case almost immediately. Then $n - m + 1 = m$, and

$$
\begin{aligned}
MSM^T &= MB \cdot \mathrm{Rev}(B)^T M^T \\
&= \begin{pmatrix}
a_1 & 1 & 0 & 0 & \cdots & 0 & 0 \\
a_2 & 0 & 1 & 0 & \cdots & 0 & 0 \\
\vdots & & & & & & \vdots \\
a_{m-1} & 0 & \cdots & 1 & 0 & \cdots & 0 \\
1 & 0 & \cdots & 0 & 1 & \cdots & 0 \\
\vdots & & & & & & \vdots \\
1 & 0 & 0 & 0 & \cdots & 0 & 1
\end{pmatrix}
\begin{pmatrix}
0 & 0 & \cdots & 0 & 0 & 0 & 1 \\
0 & 0 & \cdots & & & 1 & 0 \\
\vdots & & & & & & \vdots \\
0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\
\vdots & & & & & & \vdots \\
0 & 1 & \cdots & & & & 0 \\
1 & 0 & \cdots & & & & 0 \\
a_1 & a_2 & \cdots & a_{m-1} & 1 & \cdots & 1
\end{pmatrix} \\
&= \begin{pmatrix}
 & & & & & 1 & a_1 \\
 & & & & \iddots & & \vdots \\
 & & & 1 & & & a_{m-1} \\
 & & 1 & & & & 1 \\
 & \iddots & & & & & \vdots \\
1 & & & & & & 1 \\
a_1 & \cdots & a_{m-1} & 1 & \cdots & 1 & 2
\end{pmatrix}
\end{aligned}
$$

The determinant of this matrix can now be evaluated by reducing the final row to zeroes in all except the final column, and then expanding along that row. This gives

$$\det(S) = \det(MSM^T) = (-1)^{m-1}\left(2 - 2(a_1 + \cdots + a_{m-1})\right).$$

Lemma 4. *With a_j defined as above,*

$$a_1 + \cdots + a_{m-1} = -(m-1).$$

Proof. Plugging in the definition of a_1 and initial values for $a_m, \ldots, a_n$,

$$
\begin{aligned}
a_1 + \cdots + a_{m-1} &= (1 - a_2 - a_3 - \cdots - a_n) + a_2 + \cdots + a_{m-1} \\
&= 1 - a_m - \cdots - a_n = 1 - m.
\end{aligned}
$$

□

This completes the proof for $n = 2m - 1$.

Finally, in the case that $n = 2m$, the recursion gives $a_m = 0$. Thus, the mth row of MB has only one nonzero entry, a 1 in the first column, and is orthogonal to all other rows of MB. It follows that the mth row in MSM^T has a 1 in the mth column, and is 0 elsewhere, so this row has no effect on its determinant. Further, the conclusion in Lemma 4 also still holds, since now $a_m = 0$ implies that $a_m + a_{m+1} + \cdots + a_n = m$.

Solution 3: As in Solution 2, let m be the least integer greater than or equal to $n/2$, so that either $n = 2m$ or $n = 2m - 1$. We will define $(n+1) \times (n+1)$ matrices C and D and show that

$$CD = \begin{bmatrix} -2m & O \\ O^T & S \end{bmatrix}$$

where O denotes a row of n zeros. It will then follow that $\det S = (\det C)(\det D)/(-2m)$. We will write the entries of C and D as c_{ij} and d_{ij} where $0 \le i \le n$ and $0 \le j \le n$.

For $1 \le i \le n$ and $0 \le k \le n$, let $c_{ik} = 1$ if k is a multiple of i, and $c_{ij} = 0$ otherwise. For $0 \le k \le n$ and $1 \le j \le n$, let $d_{kj} = 1$ if $n-k$ is a multiple of j, and $d_{kj} = 0$ otherwise. Then each allowed solution of $ai + bj = n$ corresponds to a case where $c_{ik} = d_{kj} = 1$, with $k = ai$. Thus, $s(i,j) = \sum_{k=0}^{n} c_{ik} d_{kj}$, verifying the S block in the equation above for CD.

Next, we will choose column 0 of D (corresponding to $j = 0$) to be orthogonal to rows 1 to n of C, which will satisfy the O^T block of the equation for CD. Such a column must exist because these n rows can't span $(n+1)$-dimensional space. Notice that the $n \times n$ matrix $\{c_{ik}\}_{1 \le i,k \le n}$ is upper triangular, with all ones on its diagonal, so the rows of this reduced matrix are linearly independent. Thus, for the desired orthogonality, d_{00} must be nonzero, and since rows 1 to n of C span an n-dimensional space, choosing $d_{00} = 1$ uniquely determines column 0 of D. For $n - m + 1 \le i \le n$, we have $2i > n$, so $c_{ik} = 1$ if and only if $k = 0$ or $k = i$. Thus, the desired orthogonality requires that $d_{i0} = -1$ for these values of i. Also, if n is even, then row m of C is the same as row n of C except that $c_{mm} = 1$ while $c_{nm} = 0$. Thus, the desired orthogonality requires that $d_{m0} = 0$ when n is even. Then, whether n is even or odd, we have $\sum_{k=m}^{n} d_{k0} = -m$. For column 0 of D to be orthogonal to row 1 of C, all of whose entries are 1, we then must have $\sum_{k=0}^{m-1} d_{k0} = m$. We will not need to determine the individual values of d_{0k} for $1 \le k \le m-1$.

Now let $c_{0k} = d_{n-k,0}$ for $0 \le k \le n$. Notice that this makes row 0 of C (which is the reverse of column 0 of D) orthogonal to columns 1 to n of D (which are the reverses of rows 1 to n of C), satisfying the O block of the equation for CD. To complete the verification of this equation, the upper left entry of CD is

$$\sum_{k=0}^{n} c_{0k} d_{k0} = \sum_{k=0}^{n} d_{n-k,0} d_{k0} = \sum_{k=0}^{m-1} (-1) d_{k0} + \sum_{k=n-m+1}^{n} d_{n-k,0}(-1) = -m - m = -2m.$$

Next, to determine $\det C$, replace column 0 of C with column 0 of CD. Since the latter column is the sum over $0 \le k \le n$ of d_{k0} times column k of C, and $d_{00} = 1$, this replacement is a column operation on C that this does not change its determinant. The resulting matrix is upper triangular, and its diagonal consists of $-2m$ followed by n ones. Thus, $\det C = -2m$.

Finally, since D can be obtained by reversing the columns of C^T, which amounts to swapping m pairs of columns, $\det D = (-1)^m \det C^T = (-1)^m \det C = (-1)^{m+1} 2m$. Therefore, $\det S = -2m(-1)^{m+1} 2m/(-2m) = (-1)^{m+1} 2m$.